The implications of big data and privacy on competition analysis in merger control and the controversial competition-data protection interface

Wasastjerna, M.C.

2019

Wasastjerna , M C 2019 , ' The implications of big data and privacy on competition analysis in merger control and the controversial competition-data protection interface ' , European Business Law Review , vol. 30 , no. 3 , pp. 337-365 .

http://hdl.handle.net/10138/312743

publishedVersion

The Implications of Big Data and Privacy on Competition Analysis in Merger Control and The Controversial Competition-Data Protection Interface**

MARIA C. WASASTJERNA*

Abstract

The article examines the implications of big data for competition law, with a focus on personal data and the privacy concerns that such data may give rise to, especially in the area of merger control. Today, one of the biggest challenges for competition authorities in data-driven markets is how to deal with issues related to personal data and the protection of privacy in their analysis. A key question is the role of competition law in protecting consumers from potential data privacy risks arising in the context of mergers in digital markets. The article also engages with one of the currently most debated topics in the competition community, namely the competition-privacy interface, and considers how personal data in the digital economy is considered a currency in exchange for online offerings, and how a loss of privacy can be factored into quality competition. The article addresses some of the challenges with incorporating privacy as a non-price parameter into competition analysis and offers food for thought by discussing relevant methodologies to assign monetary values to personal data.

Keywords

competition law, digital economy, big data, personal data, merger control, data privacy, data protection, competition policy

I. Introduction

Competition debates associated with big data have long been on the agenda of competition authorities around the world. A few years back already, the EU Competition

* Doctoral Candidate, Faculty of Law, University of Helsinki. Visiting Academic, University of Oxford, Institute of European and Comparative Law (2018). LL.M. Georgetown Law School (2011), Magna Cum Laude, Dean's List, Fulbright-Schuman Scholar. LL.M. College of Europe (2006). E-mail: maria.wasastjerna@helsinki.fi

** This article is based on research conducted for the author's doctoral thesis in law. The opinions expressed in this article are the author's own, as are all errors and omissions. An earlier version of this article has been published in the European Competition Journal, see Maria C Wasastjerna (2018) The role of big data and digital privacy in merger review, European Competition Journal, 14:2-3, 417-444.

Wasastjerna, Maria C. 'The Implications of Big Data and Privacy on Competition Analysis in Merger Control and The Controversial Competition-Data Protection Interface'. *European Business Law Review* 30, no. 3 (2019): 337-366.

Commissioner described 'competition in a big data world' as a new antitrust frontier,[1] and it is commonly acknowledged that data can be a source of market power.[2] Now, the discourse on competition in data-driven markets has encountered privacy issues and run headlong into the world of data protection.

This is not really surprising. Although collection and analysis of data by companies is not limited to consumer data, many aspects of big data are targeted specifically at consumers. As noted by the European Data Protection Supervisor, '[n]ot all big data is personal, but for many online offerings which are presented or perceived as being "free", personal information operates as a sort of indispensable currency used to pay for those services.'[3]

Data is the price consumers pay for access to various online offerings and to platforms like Facebook and Google. How that personal information is treated by businesses is becoming a competition issue. While competition law – according to conventional thinking – is interested in data due to its economic value, data protection rules deal with personal rights, but not necessarily the market value of data. Nevertheless, the value that individuals assign to the protection of their personal data is of great importance to businesses, the legal community, and policy makers.[4]

As the amount of information about users and their preferences gathered by businesses is rapidly growing, the impact of data as a factor in competition analysis attracts increasing attention.[5] At the same time, the new EU legal framework concerning data privacy, the EU General Data Protection Regulation (GDPR), has brought data protection to the forefront of public discussion. Consumers' views on the value of personal data are also shifting in the wake of the Facebook-Cambridge Analytica scandal in which data from 87 million Facebook users was illegally harvested from the platform for electoral manipulation, now prompting citizens to wake up to their data rights and acknowledging the value of data protection.[6] The scandal pushed the power of digital platforms and privacy protection, along with political implications, to front pages around the world. Moreover, it has fuelled intellectual discourse and public engagement with the complex and highly fascinating intersection between competition law and data privacy.

Personal data is closely linked to the dignity, autonomy and privacy of individuals. The collection and use of personal information gives rise to issues concerning the

---

[1] Margrethe Vestager, *Competition in a Big Data World,* DLD 16 (Munich, 17 January 2016) <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en> accessed 5 March 2019.

[2] Autorité de la concurrence and Bundeskartellamt, *Competition Law and Data,* 11 (10 May 2016).

[3] European Data Protection Supervisor (EDPS), *Preliminary Opinion, Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy,* 6 (March 2014).

[4] Alessandro Acquisti, Leslie K John, and George Loewenstein, *What is Privacy Worth?* 42 The Journal of Legal Studies 249 (2013).

[5] French-German joint report (n 2), 11.

[6] The scandal has led to wider concerns about Facebook's entire applications ecosystem and data processing practices. MLex Comment, 'Regulatory scrutiny of Facebook data-sharing won't be limited to Cambridge Analytica privacy breach' (22 March 2018).

protection of users' (informational) privacy. In this context, an emerging question is the role of competition law in protecting consumers from potential privacy risks. This is a hot topic both in the field of antitrust and merger control, especially with the increasing number of mergers in digital markets and so-called killer acquisitions, whereby companies acquire innovative targets with the purpose of pre-empting future competition. The broader policy question concerning the interlinkage between competition and data protection is one of the most debated questions among competition law practitioners, policymakers and academia right now, and also an overarching theme of this article.

This article aims to take part in such debate and policy discourse. The article examines how concerns arising from accumulation of data and deterioration of privacy protection may be relevant for competition analysis, especially with regard to merger review. The article is structured as follows. Following the introduction, the second section introduces the emergence of big data and privacy issues in competition law, with a focus on personal data and the concerns that such data may give rise to. The third section analyses an emerging privacy dimension in merger review by looking at assessment of certain data-focused merger cases in digital markets. Next, the fourth section explores the challenges with weighing in and incorporating privacy as a non-price parameter or element in competition analysis. The article examines how personal data in the digital economy is considered both a currency in exchange for online offerings, and how a loss of privacy can be factored into quality competition. Finally, the fifth section considers a potential way forward for the challenges of dealing with personal data and privacy by discussing some relevant methodologies to estimate or assign monetary values to personal data. The article ends with some concluding remarks. Throughout the article, the interlinkage between competition and data protection law is one important theme.

II. The Emergence of Big Data and Privacy Issues in Competition Law

Increasingly, we conduct our lives online. To do this, we grant access to our personal information. During the past decade, companies such as Facebook, Amazon, Alibaba and Google (Alphabet) have sprung up and become powerful by collecting and selling user data. Facebook is described as 'the company responsible for the largest and most brazen data-collection project in human history'.[7] These data-driven businesses occupy an increasingly important role in the modern economy and no doubt have they brought about significant new innovation and benefits for consumers. Digitalization offers tremendous potential for improving people's quality of life, for doing business more efficiently, and for creating revolutionary business models.

---

[7] Jake Bittle, 'A Mark Zuckerberg Presidency Isn't Ridiculous – It's Terrifying' The Nation (18 August 2017) <https://www.thenation.com/article/a-mark-zuckerberg-presidency-isnt-ridiculous-its-terrifying/> accessed 5 March 2019.

But the emerging number of businesses that achieve extremely significant turnover based on a business model involving collection and commercial use of personal data has also spurred discussions about the role of data and its protection in economic relationships, as well as in the application of competition law to those relationships, in particular as regards the assessment of data as a factor in establishing market power. Instead of talking about monopolies in the traditional sense, the concept of data-opolies is emerging in public discourse to describe the so-called tech giants with significant market power based on data.[8]

"Big data", a concept originally used by computer scientists and today popularized among academics, regulators and politicians, is widespread across multiple industries, sectors and disciplines. However, the term has no single definition and is used in different ways.

What the concept basically tries to do is to capture recent developments in digital technologies and data-driven markets. Big data is often described as an accumulation of a significant volume of different types of data, produced at high speed from multiple sources, the handling and analysis of which requires new and more powerful processors and algorithms.[9] Big data is often also characterized by four Vs: the volume of data, the velocity at which data are collected, used and disseminated, the variety of information aggregated and the value of the data.[10] The value of big data increases with the rise of "big analytics", including algorithms that can access and analyse vast amounts of information, and the introduction of machine learning.[11] It is important to note that data is of course varied and can be divided, roughly speaking, into personal and non-personal data.[12] The GDPR provides a very broad definition of personal data as 'any information relating to an identified or identifiable individual ("data subject")'.[13]

This article is part of a larger public debate over whether modern competition policy should be updated for the age of digitalization and big data. According to *The Economist*

---

[8] Maurice E Stucke, *Should We Be Concerned About Data-Opolies*? 2 Georgetown Law Technology Review 275 (2018).

[9] See e.g., French-German joint report (n 2), 4-5.

[10] See e.g., Ariel Ezrachi and Maurice E Stucke, *Virtual Competition – The Promise and Perils of the Algorithm-driven Economy,* 15 (Harvard University Press 2016).

[11] See e.g., Ezrachi and Stucke (n 10), 15.

[12] Data is another concept lacking a common definition. In a narrower sense, the term is often used for the results of scientific experiments or measurements. But in a wider sense the concept is used to refer to (any) information, or the representation of such information, often in combination with it being stored on a computer. See e.g., definitions according to Merriam-Webster <https://www.merriam-webster.com/dictionary/data> and Oxford dictionaries <https://www.oxforddictionaries.com/definition/learner/data>.

[13] Regulation (EC) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119, 4(1).

> [d]igital information is unlike any previous resource; it is extracted, refined, valued, bought and sold in different ways. It changes the rules for markets and it demands new approaches from regulators.[14]

Whether the data economy, new technologies and evolving business practices require rethinking of competition law and policy is debated not only in public media but also the leading competition authorities in Europe and the USA are currently exploring these questions. In the end of last year, the US Federal Trade Commission (FTC) held a series of public hearings with the aim of analysing, among other, whether big technology companies have grown too big and wield too much power.[15] Citing former FTC Chairman Robert Pitofsky, who held hearings of similar kind in 1995, the agency noted that its concern is the state of American antitrust (and consumer protection) law and development in digital markets, considering technology networks, market power and entry barriers featuring online platforms, and issues concerning the use of big data.[16]

The European Commission is conducting a similar exercise in the EU through its consultation on shaping competition policy for the digital age.[17] Similarly, in the United Kingdom, the government is reviewing the impact and market influence of powerful digital technology companies and the possible need to adjust competition policy accordingly.[18]

Indeed, one of the most challenging issues for competition authorities in the digital economy is how to deal with the role of data and privacy on the other side of the coin. Data represents a core economic asset with the potential to create significant competitive advantage for companies.[19] The value of data lies, among other things, in the fact that it enables or facilitates an understanding of human behaviour by revealing, for example, patterns of information that allow companies to follow user behaviour and preferences, target their products and services accordingly and thereby monetize those services and products.[20]

---

[14] The Economist, *Fuel of the Future: Data Is Giving Rise to a New Economy* (London, 6 May 2017).

[15] US FTC Hearings on Competition and Consumer Protection in the 21st Century, Hearings on Competition & Consumer Protection, Public comment topics and process, available at <https://www.ftc.gov/policy/advocacy/public-comment-topics-process#1>. See also Gene Quinn, 'Has Big Tech Finally Become Too Big for the FTC to Ignore?' IPWatchdog (21 June 2018) <http://www.ipwatchdog.com/2018/06/21/big-tech-finally-become-big-ftc/id=98598/> accessed 5 March 2019.

[16] *Ibid*.

[17] European Commission, Call for contributions, *Shaping Competition Policy in the Era of Digitization* (12 July 2018).

[18] HM Treasury, *The Economic Value of Data: Discussion Paper* 17 (August 2018).

[19] Organisation for Economic Co-operation and Development (OECD), *Supporting Investment in Knowledge Capital, Growth and Innovation*, 319 (2013). The World Economic Forum has categorized data as a "new asset class" in its report *Personal Data: The Emergence of a New Asset Class* (January 2011).

[20] For example, in its study on the commercial use of consumer data, the UK competition authority found that consumer data can in some business sectors 'be a key competitive asset in targeting offers'

Companies are adopting business models with personal data as a key input and strategies to acquire a data advantage over rivals. As these companies with their data-driven business models strive to obtain a competitive advantage, they often look for opportunities to gain a data advantage through mergers and acquisitions.[21] When companies in digital markets merge, it can lead to a significant increase in the scope and magnitude of consumer data under the control of a single company. While this can bring about innovation and enhance consumer welfare, it may also raise privacy risks and concerns about consumer harm.

The challenge is that, conventionally, competition authorities have an economic focus in their competitive analysis that centres on the price effects of a transaction, but looks less at other, non-price, dimensions. The risk with this price-centred approach is that it could lead to some anticompetitive mergers being approved unconditionally, with a significant future cost potentially imposed on consumers.[22]

As noted above with regard to the efforts by the FTC and the European Commission, competition authorities are increasingly recognizing the importance of data in the digital economy, and are also actively contributing to the debate and addressing the issue through published reports, investigations, and sector inquiries.[23] One of the most notable examples of this development is the German Bundeskartellamt's dominance case against Facebook opened in 2016.[24] The case concerns the interlinkage between data and market power, and whether Facebook is abusing its market power by infringing data protection rules.[25] According to the preliminary finding in December 2017, the social network's breach of data protection amounts to abuse of a dominant position,[26] and the recent final decision on 6 February 2019 confirmed this view.[27] The decision by the Bundeskartellamt prohibits Facebook from making the use of its social network by users conditional on the collection of user and device related data

---

because collecting and analysing consumer data is key to gaining an accurate understanding of how to attract and retain customers. The UK Competition and Markets Authority, *The Commercial Use of Consumer Data: Report on the CMA's Call for Information*, 38, 2.88 (CMA June 2015).

[21] EDPS, *Report of Workshop on Privacy, Consumers, Competition and Big Data* 1 (11 July 2014).

[22] OECD, *Big Data: Bringing Competition Policy to the Digital Era* 17 (29-30 November 2016).

[23] Especially the German and French competition authorities have focused on competitive conditions in the digital economy and the role of data. In 2018 the German authority conducted a sector inquiry into online advertising (see press release, *Bundeskartellamt Launches Sector Inquiry into Market Conditions in Online Advertising Sector* (1 February 2018). This was followed by the French authority also conducting an online advertising sector inquiry and publishing the results in 2018, see Autorité de la concurrence, *Avis n°18-A-03 portant sur l'exploitation des données dans le secteur de la publicité sur interne* (6 March 2018).

[24] Bundeskartellamt press release, *Bundeskartellamt Initiates Proceeding against Facebook on Suspicion of Having Abused Its Market Power by Infringing Data Protection Rules* (2 March 2016).

[25] *Ibid*.

[26] Bundeskartellamt press release, *Preliminary Assessment in Facebook Proceeding: Facebook's Collection and Use of Data from Third-Party Sources is Abusive* (19 December 2017).

[27] Bundeskartellamt press release, *Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources* (7 February 2019).

and combining that information with the Facebook user accounts without the users' consent.[28]

This case is breaking ground in the interface between competition and privacy. It will surely raise many questions among competition law practitioners and policymakers and one of the most striking aspects of the German precedent is that it is entirely based on an infringement of European data protection rules enshrined in the GDPR. No doubt this case severely blurs the line between data protection and competition law.[29] But the Bundeskartellamt's case against Facebook is interesting and important in many ways, one being that so far, competition authorities have not been successful in explaining why privacy is a competition issue. Here, the German regulator makes it clear with its theory that Facebook's dominance is what allows it to impose on users contractual terms that require them to allow Facebook to track them all over. Another way of looking at it is that when there is a lack of competition, users accept terms of service that they perhaps would not in another situation, which is not truly consenting. The user consent may even be viewed as a fiction.

The case is not yet over, however, as Facebook is appealing the German decision.[30] The final outcome of the case will certainly be of outmost interest to both the competition and privacy community and its implications may be far-reaching, touching also upon societal, political and even democratic perspectives. Moreover, if Facebook loses the appeal, Germany may become a grand experiment in whether the surveillance economy is actually needed for the operation of social media.[31]

When considering the emergence of big data and privacy issues in competition law, a significant piece of guidance document is the joint report by the French and German authorities on competition law and the role of data in economic activities.[32] The study correctly notes that technological changes to the digital economy have revolutionized opportunities to collect, process and commercially use data in almost every business sector. While this may improve products and services and raise economic efficiency, the study warns that the collection and use of greater volumes of data may also raise competition concerns.[33]

For example, one concern with data in the field of merger control is that combining the datasets of two merging companies could give them an unfair competitive advantage if the combination of data prevents competitors from replicating the information

---

[28] Bundeskartellamt, *Case Summary: Facebook, Exploitative Business Terms pursuant to Section 19(1) GWB for Inadequate Data Processing* (15 February 2019).

[29] Jakob Kucharczyk, *The German FCO's Facebook Case: Blurring The Line Between Competition and Data Protection Enforcement,* The Disruptive Competition Project (8 February 2019).

[30] See Facebook's blog post responding to the ruling, 'Why We Disagree With the Bundeskartellamt' (7 February 2019) <https://newsroom.fb.com/news/2019/02/bundeskartellamt-order/> accessed 5 March 2019.

[31] Emily Dreyfuss, *German Regulators Just Outlawed Facebook's Whole Ad Business* (7 February 2019) <https://www.wired.com/story/germany-facebook-antitrust-ruling/> accessed 5 March 2019.

[32] French-German joint report (n 2).

[33] French-German joint report (n 2), 9.

extracted from it.[34] In the words of the EU Competition Commissioner, '[t]he problem for competition isn't just that one company holds a lot of data. The problem comes if that data really is unique, and can't be duplicated by anyone else.'[35] This kind of thinking is reflected in the essential facility theory in competition law.

Another concern with data is that the merged entity could increase the price at which it sells its data post-merger. It might also refuse to supply such data, for example to exclude competing providers of data analytics services, who rely on data as an input for providing their services.[36] Further, possible data-related competition restraints may arise from a merger of two companies already holding strong market positions in separate upstream or downstream markets in the form of market foreclosure for new competitors.[37]

In the context that data has been identified as the currency of the internet[38], an increase in the collection of personal data can be compared to a price increase.[39] In so-called two-sided markets, products are offered to users for free (the "free" side) and monetized through targeted advertising (the "paying" side). Crucially, personal data is the price paid by consumers in return for receiving the "free" product.[40] Data is a critical element to both these sides. Arguably, the price effectively paid by consumers is their loss of privacy.[41]

This loss of privacy extends beyond the usual advertising breaks or banner ads, as personal information and search entries are analysed by data mining software, possibly involving a much higher degree of intrusiveness. The European Data Protection

---

[34] *Ibid*, 16.

[35] Margrethe Vestager, speech, *Making Data Work for Us*, as part of Data Ethics event on Data as Power (Copenhagen, 9 September 2016).

[36] Eleonora Ocello and others, *What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case* 1 Competition Merger Brief 5-6 (February 2015).

[37] French-German joint report (n 2), 16.

[38] As long ago as in 2012 Commissioner Reding observed that '[p]ersonal data is the currency of today's digital market.' Viviane Reding, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age* at Innovation Conference Digital, Life, Design (Munich, 22 January 2012). In the recent Google Search case, the Commission noted that 'Google's flagship product is the Google search engine, which provides search results to consumers, *who pay for the service with their data*' (emphasis added). Commission press release, *Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service* (27 June 2017).

[39] OECD Big Data (n 22), 18.

[40] The vast majority of online service providers use a two-sided, or multi-sided, business model, whereby the service is offered at zero price to attract users, with online advertising generating the revenues necessary to fund the free service and make a profit. A flourishing doctrine exists on two- or multisided markets, see e.g., Jean-Charles Rochet and Jean Tirole, *Platform Competition in Two-Sided Markets* 1 Journal of the European Economic Association 990 (2003); David S Evans, *Multi-sided Platforms, Dynamic Competition, and the Assessment of Market Power for Internet-Based Firms,* University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 753 (2016); David S Evans, *The Online Advertising Industry: Economics, Evolution and Privacy* 37 Journal of Economic Perspectives (April 2009).

[41] OECD Big Data (n 22), 18.

Supervisor (EDPS) has observed that, with the rise of big data and big analytics, 'companies are able to move beyond "data mining" to "reality mining", which penetrates everyday experience, communication and even thought.'[42]

In addition to having this sort of monetary value, privacy has also been recognized as a non-price dimension of competition in the sense that companies can compete to offer greater or lesser degrees of privacy protection.[43] A degradation or loss of privacy can be viewed as a reduction in the quality of a product or service, in particular to consumers who value privacy highly.[44] It follows that, when viewing privacy as a quality dimension of a product, if an online service provider, post-merger, were to start requiring more personal information from its users or supplying their data to third parties as a condition for offering its "free" product[45], this could be seen either as a price increase or as a degradation in the quality of the product.[46]

It follows that in merger control cases, privacy might be relevant from a competition standpoint if a company benefits from strong market power in its relationship with end-users. This market power can be measured by the extent to which the company can engage in conduct 'without some benefit to consumers that offsets their reduced privacy and still retain users.'[47] A company that gains a powerful position through a merger may then be able to reinforce its market power by collecting more consumer data.[48]

Here, one possible concern is that the aggregated data resulting from a merger, when subjected to increasingly powerful big data analytic tools, may produce especially revealing pictures of consumers. In turn, this makes data breaches more far-reaching and raises the risk that data will be used to the disadvantage of consumers.[49] Further, if two horizontal competitors compete on privacy as an aspect of product quality, their merger could be expected to reduce quality.[50]

---

[42] EDPS, *Towards a New Digital Ethics: Data, Dignity and Technology* Opinion 4/2015 6 (11 September 2015).

[43] Ocello and others (n 37), 6; Howard Shelanski, *Information, Innovation and Competition Policy for the Internet* 161 University of Pennsylvania Law Review 1663, 1688 (2013); Maureen Ohlhausen and Alexander Okullar, *Competition, Consumer Protection, and the Right (Approach) to Privacy* 80 Antitrust Law Journal 36 (2015).

[44] Lisa Kimmel and Janis Kestenbaum, *What's Up with WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets* 48 Antitrust (2014).

[45] The supply of data to third parties would have to consider applicable data processing restrictions that follow from relevant data protection law, such as the GDPR.

[46] Ocello and others (n 37), 6.

[47] Shelanski (n 44), 1689.

[48] *Ibid*.

[49] Kimmel and Kestenbaum (n 45), 48.

[50] French-German joint report (n 2), 24, citing the UK Competition and Markets Authority, *The Commercial Use of Consumer Data: Report on the CMA's Call for Information,* 95 (CMA 38, June 2015).

III. Issues Regarding Data and Privacy in Digital Market Merger Cases

Competition risks related to data and privacy in digital market mergers have to some extent been examined in the past by competition authorities. Ever since the 2008 merger case of *Google/DoubleClick*[51], which received significant public attention and caught the attention of privacy advocates, the debate on the relationship between competition and privacy in the context of data has been ongoing. Now the debate has become somewhat polarized in that there are those who strongly advocate competition enforcement to prevent consumer harm in the form of privacy of consumers[52], whereas others see data as just another type of input or strategic asset, and view privacy concerns as falling outside the scope of intervention by competition enforcers.[53] In what follows, competition assessments in certain key merger cases dealing with the role of data and privacy will be examined.[54]

As we shall see, a gradual change is identifiable in the approach to a potential privacy dimension in merger cases when looking, for example, at the competition analysis in *Google/DoubleClick* and *Facebook/WhatsApp*[55], compared to *Microsoft/LinkedIn*[56] in 2016 and *Apple/Shazam* in 2018[57]. In the former cases, the Commission dismissed concerns related to privacy and held that privacy harms from the increased concentration of data resulting from the transaction were outside the scope of competition law.[58] In its review of Microsoft's acquisition of LinkedIn, however, the

---

[51] Case COMP/M.4731 *Google/DoubleClick*, C(2008) 927.

[52] Allen P Grunes and Maurice Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data,* University of Tennessee Legal Studies Research Paper No 269 (2015); Allen P Grunes and Maurice Stucke, *Debunking the Myths Over Big Data and Antitrust*, University of Tennessee Legal Studies Research Paper No. 276 (2015).

[53] See e.g., Darren S Tucker and Hill B Wellford, *Big Mistakes Regarding Big Data* 3 Antitrust Source (December 2014); Daniel Sokol and Roisin Comerford, *Does Antitrust Have a Role to Play in Regulating Big Data?* in Roger Blair & Daniel Sokol (eds), *Cambridge Handbook of Antitrust, Intellectual Property and High Tech* (Cambridge University Press, 2016); Geoffrey A Manne and Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework* CPI Antitrust Chronicle (2015). For a comprehensive list of literature reflecting both sides of the debate, see Cyril Ritter, *Bibliography of Materials Relevant to the Interaction of Competition Policy, Big Data and Personal Data* (29 September 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2845590> accessed 5 March 2019.

[54] A few words on terminology. The concepts of "privacy" and "data protection" are used interchangeably in this article. However, it is important to recognize that even though the two concepts are overlapping, strictly speaking they are also distinct from each other. While data protection law covers informational privacy, it does not incorporate all aspects of privacy, such as intrusions on physical seclusion, for example. Further, "privacy" does not capture certain aspects of data protection law, such as unconditional application to personal data in the public domain, or the rights it grants, e.g., rights of access to data, data security standards and the right to data portability. For elaboration on the link between data protection and privacy, see Orla Lynskey, *The Foundations of EU Data Protection Law,* 90 (Oxford University Press, 2015).

[55] Case COMP/M.7217 *Facebook/WhatsApp*, C(2014) 7239.

[56] Case COMP/M.8124 *Microsoft/LinkedIn*, C(2016) 8404.

[57] Case COMP/M.8788 *Apple/Shazam*, Commission decision of 6/9/2018, not yet reported.

[58] See e.g., Commission press release, *Mergers: Commission Approves Acquisition of WhatsApp by Facebook* (Brussels, 3 October 2014).

European Commission approved the deal only after Microsoft offered certain commitments, including securing competitors' access to certain data. In this merger case, the Commission explicitly noted that data privacy is an important component of competition.[59] When commenting on the merger, the EU Competition Commissioner held that 'by getting commitments from Microsoft that will keep the market open, we've helped to allow companies to compete to protect privacy more effectively.'[60] In *Apple/Shazam*, the Commission's focus was on the uniqueness of data, *i.e*. whether the integration of Shazam's and Apple's sets of user data would give the merged entity a unique advantage.

i. TomTom/Tele Atlas

Even ten years ago the Commission already recognized the important competitive implications of data in its review of TomTom's acquisition of Tele Atlas.[61] TomTom, a manufacturer of portable navigation devices and navigation software, acquired Tele Atlas, which was one of the main suppliers of navigable digital map databases, a key input for such navigation devices and software. In its review of the transaction, the Commission considered the competitive advantage of data in digital map markets. While ultimately clearing the merger, the Commission noted that the merged entity would likely have the ability to exercise market power, but lacked the economic incentives to do so.[62]

In this case, the dimension of privacy was considered and the Commission noted that 'confidentiality concerns can be considered as similar to product degradation in that the perceived value of the map for PND manufacturers would be lower if they feared that their confidential information could be revealed to TomTom'.[63] According to the Commission, confidentiality concerns as to the customer information in question could lead to reputational damage and customers considering switching products.[64] Here, privacy was looked at as a sort of quality component in the competitive assessment of the merger.

ii. Google/DoubleClick

In *Google/DoubleClick*, personal data was, probably for the first time, analysed as an asset in a merger.[65] At the time of the merger, DoubleClick was the leading provider of an ad-serving technology, which targeted ads and monitored their performance,

---

[59] Commission press release, *Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions* (Brussels, 6 December 2016).

[60] Margrethe Vestager, *What Competition Can Do – And What It Can't* at Chilling Competition Conference (25 October 2017).

[61] Case COMP/M.4854 *TomTom/Tele Atlas*, C(2008) 1859.

[62] *Ibid.*, 230.

[63] *Ibid.,* 274-276.

[64] *Ibid.*, 274-275.

[65] *Google/DoubleClick* (n 52). Joaquín Almunia, *Competition and Personal Data Protection,* at Privacy Platform Event: Competition and Privacy in Markets of Data (Brussels, 26 November 2012).

whereas Google (today Alphabet), besides being active in online search, provides online advertising space and collects large amounts of personal data.[66] The merger aimed to "combine not only the two firms' products and services, but also their vast troves of data about consumer behaviour on the internet".[67] During the merger review, several market operators and civil society groups challenged the merger on the basis of privacy.

According to privacy advocates and opponents of the merger, the mere combination of the two companies' assets, especially personal data, would allow the merged entity to achieve a market position that could not be replicated by competitors and would lead to their progressive marginalization and foreclosure.[68] For example, publishers and advertisers would have no choice but to have recourse to the merged entity.[69] Especially in the United States, the potential data consolidation raised serious concerns in the privacy community, and a complaint was filed with the FTC objecting to the merger on privacy grounds.[70]

During the merger review, the effect of the increase in the amount of personal information obtained by the combined entity was considered. However, the merger investigation found that the combination of information on search behaviour and web-browsing behaviour would not give a competitive advantage in the advertising business that could not be replicated by other players that have access to similar web-usage data.[71] Besides, the agencies decided that Google and DoubleClick were not close actual or potential competitors in any markets for online advertising or services.

The agencies' market definition has since been criticized as flawed in that the agencies missed the point that other markets were involved, and they overlooked that the acquisition of DoubleClick may have strengthened Google's position in the multi-platform online advertising market.[72] The merger was cleared unconditionally on both sides of the Atlantic, but in the United States the transaction saw one FTC Commissioner write a strong dissenting opinion claiming that the merger threatened consumer privacy:

---

[66] Commission press release, *Mergers: Commission Clears Proposed Acquisition of DoubleClick by Google* (Brussels, 11 March 2008).

[67] Pamela Jones Harbour, *Dissenting Statement in the matter of Google/DoubleClick* (20 December 2007).

[68] *Google/DoubleClick* (n 52), 359.

[69] Damien Geradin and Monika Kuschewsky, *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue* 2 Concurrences 12 (2013).

[70] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *The Electronic Privacy Information Center in the Matter of Google, Inc. and DoubleClick, Inc.* (20 April 2007).

[71] The Commission has relied on similar reasoning, where rivals' access to data post-merger was considered sufficient despite concerns regarding large data pools creating entry barriers, in cases COMP/M.6314 *Telefónica UK/Vodafone UK/Everything Everywhere/JV (Mobile Wallet JV)*, C(2012) 6063; COMP/M.7023 *Publicis/Omnicom*, C(2014) 89, and COMP/M.7337 *IMS/CEGEDIM*, C(2014) 1025.

[72] See European Parliament, *Challenges for Competition Policy in a Digitalized Economy* Study for the ECON Committee, Directorate-General for Internal Policies, Economic and Monetary Affairs 54 (2015).

> [i]f the Commission closes its investigation at this time, without imposing any conditions on the merger, neither the competition nor the privacy interests of consumers will have been adequately addressed.[73]

In the EU, the Commission, in its approval of the deal, made it clear that it assessed the merger only under EU competition law and that the decision was without prejudice to the obligations of the merging parties under privacy legislation.[74]

iii. Facebook/WhatsApp

The Commission largely echoed its *Google/DoubleClick* analysis in the subsequent review of online social networking company Facebook's acquisition of mobile messaging company WhatsApp, clearing the merger unconditionally in 2014.[75] Here, the competition analysis focused on the market for advertisements and the potential harm to advertisers resulting from an increase in Facebook's market power through increased data collection capability. The outcome of the Commission assessment was that even if Facebook were to collect and use data from WhatsApp for advertising purposes, valuable user data would remain available to competitors beyond Facebook's exclusive control.

However, the Commission did not examine whether personal data from end users may be collected to a greater extent due to the combination.[76] This illustrates the challenges of examining the impact of a merger on two or multisided digital markets, where competition authorities at times consider the implications of a merger only on the advertising side, ignoring the impact on the free side, which may make consumers worse off. Here, the Commission considered the data concentration only on the advertising side of the market but did not analyse whether consumers might be harmed if Facebook were to start collecting and using data from WhatsApp users. Concerns about Facebook holding a significant amount of data were dismissed as strictly a privacy issue, outside the scope of competition law.[77]

---

[73] Pamela Jones Harbour, *Dissenting Statement in the Matter of Google/DoubleClick* (20 December 2007) 1. Since leaving the agency, former Commissioner Harbour has continued to urge enforcers to develop a more sophisticated analytical framework for evaluating the antitrust implications of privacy and personal data, see Pamela Jones Harbour, *The Transatlantic Perspective: Data Protection and Competition Law* in Hielke Hijmans & Herke Kranenborg (eds), *Data Protection Anno 2014: How To Restore Trust?,* 225 (Oxford: OUP 2014); Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets* 76 Antitrust Law Journal 769 (2010).

[74] The FTC in its closing statement also noted that 'privacy considerations, as such, do not provide a basis to challenge this transaction'. However, the FTC explicitly recognized that privacy can be a non-price dimension of competition, and that the FTC has the authority to act where a transaction is likely to reduce competition on that basis. Kimmel and Kestenbaum (n 45), 48.

[75] *Facebook/WhatsApp* (n 56).

[76] *Ibid.*, 164: 'For the purposes of this decision, the Commission has analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof.'

[77] *Ibid*.

At the time, lively discussion, controversy and objections surrounded the merger review, as well as Facebook's compliance with data protection rules and privacy. The Commission chose not to deal with the question whether merger clearance should be conditional on strict compliance related to data protection[78], but stated, as it had in *Google/DoubleClick*, that any privacy-related concerns arising from the increased concentration of data as a result of the transaction fall within the scope, not of EU competition rules but of EU data protection rules.[79] While it recognized privacy as one of many parameters of competition between consumer communications apps, and while noting that users increasingly value privacy and security, the Commission concluded that most consumer communications apps on the market do not compete mainly on privacy features.[80]

During the merger review, Facebook had pledged that it would not merge the two user-bases. However, two years after being granted unconditional clearance, it started doing so in 2016.[81] This development led the Commission to question Facebook about its privacy policy changes and Finally, in December 2016, the Commission sent Facebook a formal statement of objections for allegedly having provided incorrect or misleading information during the 2014 merger review.[82] The outcome of the investigation was that Facebook received a hefty fine amounting to €110 million – the first time a company had ever been fined for disclosures since the entry into force of the 2004 Merger Regulation.[83] The Commission has stressed that the decision is unrelated to privacy or data protection issues[84], holding that the fact '[t]hat they didn't merge

---

[78] In its review of the merger in the United States, the FTC took another approach and sent a letter to the merging parties urging them to continue to honour the promises made to consumers with respect to WhatsApp's privacy policies as well as public statements about privacy made when the transaction was announced. Failure to honour these promises could constitute deceptive or unfair practices in violation of the FTC Act. See Letter from Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission, to Erin Egan, Chief Privacy Officer, Facebook, Inc, and Anne Hoge, General Counsel, WhatsApp Inc (20 April 2014).

[79] *Facebook/WhatsApp* (n 56), 164.

[80] *Ibid.*, 174.

[81] When the acquisition was announced, WhatsApp told users that its messaging product and Facebook's existing Messenger app would continue to operate as standalone applications and the transaction would not change anything in terms of the treatment of personal data by WhatsApp. As a response to privacy concerns raised about the transaction at the time, Facebook's Chief Executive Mark Zuckerberg was reported as proclaiming that Facebook was "absolutely not going to change plans around WhatsApp and the way it uses user data". See Facebook, *WhatsApp blog* (19 February 2014) <https://blog.whatsapp.com/499/Facebook> accessed 5 March 2019; WhatsApp blog, *Why we don't sell ads* (18 June 2012) <https://blog.whatsapp.com/245/Why-we-dont-sell-ads?> accessed 5 March 2019; Kimmel and Kestenbaum (n 45), 51.

[82] According to the charges, the technical possibility of automatically matching Facebook users' IDs with WhatsApp users' IDs already existed in 2014, contrary to Facebook's statements at the time. See Commission press release, *Mergers: Commission Alleges Facebook Provided Misleading Information about WhatsApp Takeover* (Brussels, 20 December 2016).

[83] Commission press release, *Mergers: Commission fines Facebook €110 million for Providing Misleading Information about WhatsApp Takeover* (Brussels, 18 May 2017).

[84] *Ibid*.

data wasn't the decisive factor when the merger was approved',[85] noting, however, that this 'was still a part of the decision'[86].

iv. Microsoft/LinkedIn

Data and privacy were central in the Commission review of Microsoft's acquisition of the LinkedIn professional social network in 2016.[87] Critics of the deal, such as internet software company Salesforce – whose own bid to buy LinkedIn failed – argued that acquiring LinkedIn would give Microsoft exclusive access to data on how the social network's 450 million users interact. This, so the argument went, would create an unfair advantage over rivals through restricting access to that information, which pre-merger was only available to LinkedIn.[88]

The outcome of the Commission's merger review led to commitments being required from Microsoft to protect competition between professional social networks, in three respects. Firstly, for five years, PC manufacturers and distributors can choose whether or not to install LinkedIn on Windows. Secondly, competing networks will continue to enjoy certain interoperability with Microsoft products. Thirdly – and importantly – competing networks will be granted access to data stored in Microsoft Cloud.[89]

In its assessment, the Commission considered the protection of privacy and explicitly noted that data privacy can be an important parameter of competition and a driver of customer choice.[90] Accordingly, privacy can be taken into account in a competition assessment to the extent that consumers see privacy as a significant factor of quality, and the merging parties compete with each other on this factor. In this instance, the Commission concluded that data privacy, as an important dimension of competition between professional social networks on the market, could have been negatively affected by the transaction.[91]

---

[85] Some have been doubtful of this: '[N]ow, it [the Commission] claims to have received "incorrect or misleading information" at the time. We dare say that the Commission was probably the only party actually misled […]' and 'it [the Commission] has merely bent over backwards to emphasise just how unrelated this new investigation is to its 2014 merger clearance decision.' Rating Legis blog, 'Merry Christmas, WhatsApp Users' (23 December 2016) <http://ratinglegis.eu/en/eu-commission-looks-at-facebook-whatsapp-deal-again/> accessed 5 March 2019.

[86] See n 85.

[87] *Microsoft/LinkedIn* (n 57).

[88] Nick Wingfield and Kate Benner, *How LinkedIn Drove a Wedge Between Microsoft and Salesforce* (New York Times, 5 November 2016). Also relevant for the case was whether Microsoft's exclusive use of LinkedIn's metadata, in conjunction with artificial intelligence software under development by companies, including Microsoft, could give rise to an unfair competitive advantage. See Richard Waters, *Data Mining: Microsoft-LinkedIn Deal Raises New Competition Concerns* (Financial Times, 3 November 2016).

[89] Commission press release, *Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions* (Brussels, 6 December 2016). Competition authorities elsewhere, such as in the United States, Canada, Brazil and South Africa, approved the transaction unconditionally.

[90] *Microsoft/LinkedIn* (n 57) 350, n 330.

[91] *Ibid*.

v. Apple/Shazam

In 2018, the Commission accepted referral requests from Austria, France, Iceland, Italy, Norway, Spain and Sweden concerning the proposed acquisition by Apple of Shazam, a developer and distributor of music recognition apps for smartphones, tablets, and personal computers. The Commission opened an in-depth merger investigation and in its assessment focused especially on potential anticompetitive effects coming from Apple's access to commercially sensitive data about customers and rivals regarding digital music streaming services. The transaction was approved by the Commission after a careful review of the acquisition of commercially sensitive data sets, here Shazam's user and music data. The *Apple/Shazam* case constitutes an important addition to the series of merger cases involving the use of customers' personal data and contributes to the discussion on rethinking competition law in the digital economy.[92] One takeaway is the challenge of assessing market power in the presence of non-monetary pricing.[93] In its merger analysis, the Commission notes the inconvenience in using market shares as a proxy for market power in fast-growing sectors that are characterized by frequent market entry and short innovation cycles.[94] However, while acknowledging the inadequacy of market shares as a measurement of market power and recognizing the existence of a problem with its estimation of market power, the Commission does not conduct a more holistic inquiry that would lead to more solid conclusions.[95]

The *Apple/Shazam* case does confirm that data is market power and constitutes an important consideration in competition law. When commenting on the decision, the EU Competition Commission noted that

> *"*Data is key in the digital economy. We must therefore carefully review transactions which lead to the acquisition of important sets of data, including potentially commercially sensitive ones, to ensure they do not restrict competition."[96]

As the above review of some data-focused merger cases illustrates, competition authorities' traditional way of examining transactions is often through the lens of price competition. Authorities tend to avoid entering into deeper analysis of harm when such is harder to quantify, such as the impact of a merger on privacy. This price-centric approach and straightforward analysis may still work well when datasets are acquired and fairly transferred, such as in *TomTom/Tele Atlas*, but the competition analysis becomes more difficult in the context of more data-driven strategies where the product or service is free, or non-monetary, with the "cost" of consumer

---

[92] For an insightful discussion on the Commission decision, *see* Nicolo Zingales, *Apple/Shazam: Data Is Power, But Not A Problem Here,* Competition Policy International (December 2018).

[93] *Ibid.*, 5.

[94] Apple/Shazam (n 59), para. 162.

[95] Nicolo Zingales (n 96), 5.

[96] Commission press release, 'Mergers: Mergers: Commission clears Apple's acquisition of Shazam' (Brussels, 6 September 2018).

privacy. *Google/DoubleClick* serves as a good example of such a scenario and critics argued that the combination of the companies' valuable sets of user information amounted to a significant reduction in the quality of the search product for the many millions of individuals with high privacy preferences.[97]

Another illustrative example is *Facebook/WhatsApp*. In this case, the Commission, years after its clearance decision, decided to take action against Facebook – eventually imposing a heavy fine – in connection with the combined entity's privacy degradations. In this regard, a question that arises is whether consumers would actually be better off today had the Commission also assessed the impact of the merger on the free side of the market, and considered the implications for consumers in addition to advertisers, which would have required an analysis that looks at possible possible negative effects on non-price parameters, such as privacy.

The answer to this question is not straightforward, especially as incorporating a potential privacy dimension into competition analysis is not without criticism. Opponents declare, for example, that privacy concerns are not within the scope of competition authorities' powers.[98]

The *Apple/Shazam* case highlights this complex interaction of competition and privacy or data protection law. One of the specific concerns that led the Commission to open a second phase investigation was inextricably linked to data protection law, namely whether Apple could use information collected through Shazam in order to identify customers of Apple Music' s rivals, and ultimately target them with advertising or marketing campaigns. The Commission's assessment did not enter into any detail on the competition-privacy interface and whether data protection law prevents such targeting, an analysis which would depend on the specific conditions regarding personal data processing, as well as conditions on transparency and safeguards available to data subjects. The analysis contained in the Commission's decision in this respect is limited to noting "without prejudice of the assessment by the competent data protection authorities" that Shazam's terms of service and privacy notice "appear to inform" on processing of customer information that Shazam collects.[99]

The complex issue of the interlinkage between competition and data protection will be discussed in the following sections of this article. The focus of the next section is on examining the challenges and practical limitations of incorporating privacy as a dimension of competition law. This is done by looking at some practical possibilities of measuring potential privacy harms in competition analysis.

---

[97] Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis* (Center for American Progress, 19 October 2007).

[98] Sokol and Comerford (n 54), 6.

[99] *Apple/Shazam* (n 58), para. 231.

IV. The Controversial Competition-Data Protection Interface and the Challenge of Weighing in Privacy

The interface between competition and privacy is perceived as problematic partly due to the fact current competition law and policy is pre-dominantly centred on price competition. Some competition scholars and theorists even hold that without prices there can be no markets, and consequently no market power. An overly price-centred approach to competition risks overlooking significant welfare harms relating to non-price dimensions of competition, such as privacy. This approach also denotes that competition includes both price and non-price parameters.

In this regard, it is worth recalling the basis of competition theory, namely that at its simplest, the benefits of competition are lower prices, better products and services, wider choice and greater efficiency. The main parameters of competition are thus price, quality, quantity, choice and innovation.[100] Acknowledging that competition consists of both price and non-price elements, it is fundamental that one key non-price aspect of competition is quality. Quality is a key consideration – in addition to price – for consumers when determining whether to buy a product or service.[101]

In today's online markets, where products and services are commonly offered to consumers at zero-price, competition is increasingly focusing on non-price elements, such as quality.[102] Quality also fosters innovation and economic growth. As a broad notion, the concept of quality includes privacy protection and thus privacy can be viewed as a parameter of non-price competition.[103] As noted by *Ohlhausen* and *Okuliar*, 'privacy protection has emerged as a small, but rapidly expanding, dimension of competition among digital platforms'.[104]

Generally in competition law and specifically in merger analysis, competition analysis adopts a price-centric approach that focuses on factors that are easily measurable, such as short-term pricing effects and short-term productive efficiencies.[105] This price-centric approach is not optimal in data-driven markets, where products and services are offered at zero price and consumers are used to not paying for products and services – other than with their data.[106] As illustrated above in the review of some

---

[100] See e.g., C-413/06 P *Bertelsmann* [2008] ECR 4951, para. 121, T-168/01 *Glax*o [2006] ECR II 2969, para. 106, and many other judgments, including C-413/14 *Intel* [2017] 632, para. 134.

[101] OECD, *The Role and Measurement of Quality in Competition Analysis,* 5 (28 October 2013).

[102] See e.g., Case COMP/M.6281 *Microsoft/Skype*, C(2011) 7279, 81 (noting that '[s]ince consumer communications services are mainly provided for free, consumers pay more attention to other features' and '[q]uality is therefore a significant parameter of competition'.

[103] EDPS, Preliminary Opinion, '*Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy*' (March 2014) 6.

[104] See Maureen K Ohlhausen and Alexander P Okuliar, *Competition, Consumer Protection, and the Right (Approach) to Privacy* 80 Antitrust Law Journal 133 (2015).

[105] Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (Oxford University Press 2016).

[106] Stucke and Grunes (n 108), 107. See also Michal S Gal and Daniel L Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement,* NYU Law & Economics Working Papers,

merger cases, data-focused mergers can differ from other more conventional mergers in that they raise concerns about degrading consumers' privacy. In these cases, the potential harms are more difficult to quantify. However, this does not make them less significant. The challenge is to consider the intangible harm that comes from invasions of privacy and to measure privacy as a harm in a competitive assessment.

Although price competition dominates competition analysis in the EU and the United States, it is worth recalling that the applicable legal framework and merger guidelines do not limit the competition authorities to focus only price effects in merger analysis. For example, the EU Horizontal Merger Guidelines expressly state that one of the effects to be analysed in merger control is the effect on quality, which effectively places the harm caused by a reduction in quality on a par with an increase in prices:[107]

> Effective competition brings benefits to consumers, such as low prices, high quality products, a wide selection of goods and services, and innovation. Through its control of mergers, the Commission prevents mergers that would be likely to deprive customers of these benefits by significantly increasing the market power of firms.[108]

Similar to the merger guidance, guidance from the European Commission on the assessment of agreements and unilateral conduct also includes the notion of quality as a factor in competitive analysis. The Horizontal Guidelines set out how various kinds of cooperation agreements between actual or potential competitors can have negative or positive effects on product quality.[109] The Vertical Guidelines contain similar guidance regarding distribution agreements.[110] Besides, the General Guidelines concerning agreements contain guidance on how to assess quality improvements in analyzing efficiencies,[111] and the Market Definition Notice provides information on how quality considerations can be relevant for defining the relevant product market.[112] Thus, the wording in the Commission's various guidance documents as such goes to show that competition analysis can look beyond price-related harms and take

---

Research Paper No. 14-44 (January 2015); John Newman, *Antitrust in Zero-Price Markets: Foundations* 164 University of Pennsylvania Law Review 149 (2015) (discussing how traditional antitrust theories and analytical frameworks have failed to develop an adequate response to zero-price markets).

[107] OECD Quality Report (n 103), 83.

[108] *Commission, Guidelines on the Assessment of Horizontal Mergers under the Council Regulation on the Control of Concentrations Between Undertakings* [2004] OJ C 31/03, 8. See also Commission, *Guidelines on the Assessment of Non-Horizontal Mergers Under the Council Regulation on the Control of Concentrations Between Undertakings* [2008] OJ C 265/07, 10.

[109] *Commission Guidelines on the application of Article 101 of the of the Treaty on the Functioning of the European Union*, 1.

[110] *Commission Guidelines on Vertical Restraints*, OJ [2010] C 130/01, 1.

[111] *Commission European Commission, Guidelines on the application of Article 81(3) of the Treaty*, 97.

[112] Notice on the definition of relevant market for the purpose of Community competition law [1997] OJ C372, 5.

into account the element of quality, which, as a broad notion, includes a privacy dimension.

It seems conceptually clear that the concept of quality includes privacy protection, and – as discussed above in the context of *Microsoft/LinkedIn* and *Apple/Shazam* – an intellectual shift has occurred in the European Commission's approach to privacy and factoring in privacy as a quality factor in a case or merger. Also in praxis, competition authorities have noted the importance of quality as a competitive feature when a product or service is offered for free; that in instances where price is constrained, quality becomes more important.[113] Nevertheless, while it may be conceptually clear that privacy can be an element in quality-based competition, the challenge lies in making this approach fully operational. The issue is that consumers attach widely different values to privacy, which confounds rigorous analysis. Even if most consumers would probably agree that a reduction in product quality is undesirable (at least at constant prices), consumers will differ greatly in the value that they attach to privacy protection exceeding the legal standard that all service providers are obliged to respect.[114]

Another challenge with privacy as a quality dimension is that despite the importance of quality being recognized as an important competitive element and the legal framework allowing for non-price considerations in competition analysis, competition policy is often still driven by how competition affects price. Although recent decisional practice reflects an awakening intellectual shift within the Commission and activities by national competition authorities signal increasing attention towards data privacy hams, the focus is still often on price impact in competitive assessment.

For example, when assessing a merger, the competition authorities inquire whether the transaction will likely give the parties the power to raise the price of the product or service price above competitive levels. The so-called Small, but Significant, Non-transitory Increase in Price (SSNIP) test is used to assess customer reactions to a price increase in the range of 5 to 10 per cent by a hypothetical monopolist (also known as the hypothetical monopolist test).

A problem arises, though, since in the context of digital products or services that are offered to users for free, the SSNIP test cannot be applied, as noted by Commission officials in the setting of the *Facebook/WhatsApp* merger.[115] This is because the practical implication of a zero price is that some of the standard tools of market definition and market power analysis break down as a pure mathematical matter: '5 percent of nothing is nothing, and because the nature of the product may be such that the hypothetical monopolist would still find it profit-maximizing to price at zero.'[116]

In any event, achieving a precise definition of quality for a given product is a complex task in competition investigations for many reasons. These would include factors

---

[113] *Microsoft/Skype* (n 104) 81; COMP/M.5727 *Microsoft/Yahoo* C[2010] 1077.

[114] Ohlhausen and Okuliar (n 107) 133.

[115] Ocello and others (n 37), 3.

[116] Stucke and Grunes (n 108), 117, citing David S Evans, *The Antitrust Economics of Free* 22 Competition Policy International (Spring 2011).

such as the subjective features that contribute to a perception of quality by customers; the multi-dimensional nature of quality; and the absence of measurable variables.[117] And even if some quality-related features are measurable, the overall perception of product quality is often based on a combination of several features.[118] Therefore, assessing quality is often a complex and imprecise exercise in itself that involves weighing evidence which is often of a subjective nature, such as different customer perceptions.

As quality is often difficult to measure and define, quality considerations in practice are commonly assessed by means of customers' and competitors' views. These are collected during market investigations or as documentary evidence, such as internal analysis or in-house surveys. The possibility to use more exact quantitative tools is – in contrast to a price-centred assessment – more limited.[119]

In some cases, quality, or perceived quality, correlates with the price positioning of a given product or service. In other words, at times consumers assess quality using price as a proxy, in that you get what you pay for (a decrease in quality for a given lower price).[120] The more customers perceive a product or service as being highly qualitative – by way of its proper characteristics or by marketing – the more they are willing to pay for it and the more the observed prices of the given products differ.[121]

Ezrachi and *Stucke* argue that competition authorities rely on several heuristics to circumvent the challenges they face in appraising quality. Instead of attempting to quantify the impact of a merger on quality, the agencies rely on heuristics concerning, for example, consumers' ability to accurately assess quality differences and imperfect information flows regarding quality. The problem with heuristics is that they break down, because they fail to accurately reflect the relationship between competition and quality or to consider that market realities are more complex.[122]

In particular, problems arise with the heuristic regarding price correlation in digital markets with zero-price products and services.[123] In these instances, personal information is exchanged for products or services that are free, or that do not reflect the value of the information. This creates a challenge in identifying at what point the requirement for consumers' disclosure of personal data for online transactions – without improving them or lowering their price – is commensurate with the value of the data, and is therefore anticompetitive. In other words, when does the price become too high.

---

[117] OECD Quality Report (n 103), 78-79.

[118] *Ibid*. Taking cars as an example, the number of measurable variables that customers may take into account when assessing quality is huge and quite complex, ranging from speed, emissions, acceleration, and consumption to the precise parameters of individual components.

[119] *Ibid*.

[120] Ariel Ezrachi and Maurice E Stucke, *The Curious Case of Competition and Quality* 3 Journal of Antitrust Enforcement 227-257 (2015).

[121] OECD Quality Report (n 103), 79. For example, price levels can be indicative of the (perceived) quality positioning of brands, e.g., with watches, where luxury brands are several times more expensive than technically comparable "regular" watch brands.

[122] Ezrachi and Stucke, Competition and Quality (n 123), 227-257.

[123] *Ibid*.

The EU Competition Commissioner has stated that consuming free services against disclosure of data 'doesn't have to be a problem, as long as people are happy that the data they share is a fair price to pay for the services they get in return.'[124] This is not really helpful, though, as what constitutes a "fair" price, just like the concept of "fairness", is highly subjective and open to various interpretations.[125] If the agreement to disclose and permit personal data processing had a price tag, it would fit more easily within the conventional competition law framework. But, because most online offerings are free, price effects in the traditional sense are absent. Consumer decisions and preferences may reflect whether competition in the marketplace exists, but they cannot determine whether certain behaviour is anticompetitive. For example, if consumers are charged high prices as a result of a merger, they would still pay what they believe a product or a service is worth to them.[126]

Although the significance of quality and privacy as non-price parameters of competition might be recognized, competition authorities may not currently have the tools and analytical schemes for assessing these non-price dimensions. Consequently, considerations regarding quality and privacy are not always sufficiently present in current competition analysis. Due to the unfamiliarity and difficulty in measuring and appraising quality, little attempt has been made to quantify, for example, how mergers may lessen quality. To address this gap, it has been suggested that competition authorities would use the SSNDQ test, which stands for a Small, but Significant, Non-transitory Decline in Quality.[127]

However, for many products and services, quality attributes are of a subjective nature, complex and difficult to measure. Therefore, the test is in practice difficult, if not impossible, to apply, because of the lack of a single parameter that defines quality. For the SSNDQ test to work, the quality component would have to be measurable, objective, transparent and well accepted.[128] The SSNDQ test may work in industries with well-accepted metrics of quality, such as health care. For example, *Ezrachi* and *Stucke* discuss the use of the SSNDQ test by the UK competition authority in its review of hospital mergers.[129]

Just like the difficulty with applying the SSNDQ test to assess a merger's implications on quality, the test has limitations in terms of privacy. Just like quality, privacy is subjective and lacks quantifiable metrics. Due to the subjectivity of consumer preferences about privacy, the SSNDQ test has practical limitations for measuring a potential privacy degradation or the degree of privacy protection generally. The element of subjectivity makes privacy – like quality more generally – harder to define

---

[124] See Margrethe Vestager speech (n 36).

[125] On the currently debated concept of fairness in EU competition law, see e.g., Maurits Dolmans and Wanjie Lin, *Fairness and Competition Law: A Fairness Paradox* 4 Concurrences Review (November 2017); Harri Kalimo and Klaudia Majcher, *The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace* 42 European Law Review 210 (2017).

[126] This is shown in demand curves by competition economists for any market.

[127] OECD Quality Report (n 103) 164.

[128] Ezrachi and Stucke (n 10).

[129] *Ibid*.

and measure than price, which mirrors the lack of a commonly accepted analytical framework and consequent superficial treatment at times by competition authorities.[130] Generally, the economic analysis of privacy has evolved over time, but characterizing a single unifying economic theory of privacy has proven hard. This is partly due to privacy issues of economic relevance arising in widely diverse contexts.[131]

As mentioned, applying the SSNDQ test to assess privacy involves inherent difficulties, due to the subjectivity of consumer preferences about privacy and the lack of quantifiable metrics. However, despite the unavailability of a commonly accepted analytical framework for privacy, some studies on the value of personal data look at different methodologies to measure and estimate the monetary value of personal data.[132] Many of these studies acknowledge that while personal data is creating economic and social value at an increasing pace, estimating the value being generated is difficult. This is because not only is a huge amount of data being generated, but personal data is used in so many different situations for numerous purposes.[133]

When commenting on the *Google/DoubleClick* decision, former EU Competition Commissioner Almunia predicted that, while the Commission had not yet at that time encountered a merger where it suspected that personal data could be used to breach EU competition law, this did not mean that it could not happen: '[i]n time, personal data may well become a competition issue.'[134] Indeed, looking at where we are today, this prediction seems to have come true, at least conceptually. What remains to be seen is how this approach to privacy as an element in competition can be become practically operational in competition enforcement. In this regard, the next section considers the way forward by considering potential measuring tools for competition authorities to use in their assessment of privacy as a competition dimension.

V. Addressing the Challenges of Measuring Data and Privacy

To address some of the challenges of dealing with personal data and privacy, in the following some relevant methodologies and estimation techniques for assigning monetary values attached to personal data are discussed. The idea is that these methodologies for valuing personal data could be used as basis to further develop the economic and legal analysis of privacy and to provide a measuring tool for competition authorities with the increasing confrontation with privacy issues in competition cases.

Market prices for data. As noted, consumers at times assess quality using price as a proxy. The same logic applies to assessing the value of personal information. The

---

[130] Stucke and Grunes (n 108), 266.

[131] For further reading on the economics of privacy, see Alessandro Acquisti, Curtis R Taylor and Liad Wagman, *The Economics of Privacy* 52 Journal of Economic Literature 2 (2016).

[132] See in particular OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value,* Digital Economy Paper No 220, 7 (2013).

[133] *Ibid.*, 2.

[134] Almunia speech (n 66).

most direct way to approach the value of personal data is probably to evaluate the market prices at which personal data are legitimately offered and sold. The values are imprecise as they only represent the price of data sold in a specific context to one participant and do not show the total "earnings" of the data over time. They do, however, offer a market-based measurement based on the intersection of supply and demand. Examples of prices for personal data in the USA can range from USD 0.50 for a street address, USD 2 for a date of birth, USD 8 for a social security number, USD 3 for a driver's license number and USD 35 for a military record.[135] These are only estimates but give some insight into the relative market values of different pieces of personal data.

Financial results per data record. According to the OECD study on the economics of personal data, financial results are another principal way of assigning monetary value to personal data.[136] Financial results include market capitalizations, revenues or net income per individual record. Market capitalization as an approach is suitable for companies whose business models are based primarily on personal data. However, market capitalization data leads to valuations that can fluctuate considerably. For example, the implied market capitalization or valuation per Facebook user fluctuated between USD 40 and USD 300 per user at different times between 2006 and 2012.[137] The fluctuations are influenced to a large extent by other economic factors and not solely by the monetary value of the underlying data.[138]

Revenue or net income per record/user is arguably a more stable measure of the annual market value of personal data. For example, Facebook and Experian, two companies whose business models are based on personal data, have annual revenues per record/user of roughly USD 4-7 per year. While imprecise, the data can serve as a useful point of reference. It should be noted, however, that only at the level of net profit per record is added economic value actually measured.[139]

Costs of data breach. Another approach to considering the monetary value of personal data is through an assessment of the economic costs of a data breach. This methodology includes measures of the cost to individuals who have their identities stolen or the costs to companies when a data breach occurs. The costs associated with the loss and misuse of personal data can give some indication of its value. A drawback of this approach is that reported figures vary widely.[140] Moreover, it does not measure the value of the underlying data but rather the monetary cost of a breach on a per-record basis. For example, the data, or data security breach concerning the Sony PlayStation Network and Sony Online Entertainment in 2011 resulted in the exposure of 103 million records. According to Sony executives, the data breach would cost the

---

[135] OECD, *Economics of Personal Data* (n 35), 25-27. The examples are taken from the OECD study at the time of writing the report (2013).

[136] *Ibid.*

[137] *Ibid.*, 20-25.

[138] *Ibid.*

[139] *Ibid.*

[140] *Ibid.*

company at least USD 171 million (USD 1.7 per record).[141] It does not, however, cover loss in company reputation, brand impact and other indirect and opportunity costs.

Willingness to pay to protect through insurance. Another way to put an economic value on personal data is to understand how much someone would be willing to pay to protect that data in the form of insurance. This can also be seen in markets in the form of insurance policies to protect against identity theft. For example, the data broker Experian sells an identity-theft protection service called ProtectMyID for USD 155 per annum in the USA. It is interesting to compare this figure with the mentioned examples of average revenue per record (USD 6.42) and market capitalization per record (USD 19.24) for some perspective on the difference between measures.[142]

Economic experiments and surveys. Another way to assign economic value to personal data is to conduct economic experiments and surveys that extract the price that companies would have to pay individuals for them to give up some of their personal information. Several experimental studies have attempted to quantify individual valuations of personal data in diverse contexts.[143] Research in this area is still developing, as the notion of individual valuation of privacy is complex and extremely context-dependent, which makes it challenging to analyze in a laboratory setting.[144] However, the notion of individual valuation of privacy can also be irrational, which brings even more complexity to the issue and may require insights based on behavioural economics.

Moreover, according to research results, there is a difference between individual valuation of personal data and individual valuation of privacy in the sense that people tend to differ with respect to their individual valuation of personal data (the amount of money sufficient for them to give away personal data) and their individual valuation of privacy (the amount of money they are ready to spend to protect their personal data from disclosure). Generally, the proportion of consumers who will reject an offer to obtain money in exchange for reduced privacy is larger than the proportion of consumers who will accept an economically equivalent offer to pay money in

---

[141] *Ibid*.

[142] It is, however, questioned whether services that offer to protect and rectify the theft of personal data are actually effective and therefore can be viewed as a valid instrument of measurement.

[143] Numerous empirical studies focus on both the valuation of personal data and the valuation of privacy. Examples include Kai-Lung Hui, H-H Teo, S-Y Lee, *The Value of Privacy Assurance: An Exploratory Field Experiment* 31 MIS Quarterly 19-33 (2007); R Chellapa and RG Sin, *Personalization Versus Privacy: An Empirical Examination of the Online Consumers' Dilemma* 6 Information Technology and Management 181-202 (2005); L Wathieu and A Friedman*, An Empirical Approach to Understanding Privacy Valuation,* Proceedings of the Fourth Workshop on the Economics of Information Security (WEIS (2005); D Cvrcek et al, *A Study On The Value Of Location Privacy,* Proceedings of Workshop on Privacy in the Electronic Society, 109-118 (WPES 2006); S Spiekerman, J Grossklags and B Berendt, *E-privacy* in *2nd generation E-Commerce ACM Conference on Electronic Commerce* (EC'01) 38-47 (2002).

[144] However, economic experiments and procedures are well described in the literature, see e.g., JH Kagel and A E Roth, *The Handbook of Experimental Economics* (Princeton University Press, 1997) .

exchange for protection of privacy.[145] According to *Hui* and *Png*, the difference between the individual valuation of personal data and the valuation of privacy could help explain some of the disparate findings from empirical studies.[146]

Empirical studies also show that both the valuation of privacy and the valuation of personal data are sensitive to contextual effects. Studies suggest that even supposedly privacy conscious individuals are likely to share their personally sensitive information with strangers.[147] A strict application of the economics principle of "revealed preferences" would invite the conclusion that people do not care about their privacy or their personal data.[148] Efforts to explain this inconsistency involve using techniques developed by behavioural economics that weigh in and take into account relevant context, psychological and individual motives in economic settings. Studies based on behavioural economics reveal how significantly the valuation of privacy and the valuation of personal data can be affected by contextual effects that arguably should play a limited role in decision making.[149] These studies also demonstrate the complexity of individual privacy preferences by examining the underlying privacy and personal data valuations, finding that these are not normally or uniformly distributed, but clustered around extremes and focal points.[150]

It should be acknowledged that these different approaches for assigning monetary values to personal data and the economics of personal data and privacy have some caveats or limitations. Importantly, the methodologies reflect a purely monetary perspective in that they do not take into account the indirect impact of use of personal data on the economy or society. Further, they produce monetary estimates of values that are context dependent, and they may lead to biased results if relying solely on one specific approach. In addition, challenges arise with concepts and definitions, due to inherent difficulties in determining precisely what amounts to personal data, and in comparing different proxies for personal data such as "records" or "users."[151]

Markets are likely to evolve in which individuals control and sell their own data. As mentioned, online users and consumers generally are more and more waking up to how technology companies with data-driven businesses are using and monetizing online user data in ways that which may raise privacy risks. New developments are on the horizon that could produce novel valuations of personal data and shed further light on their market valuations. For example, some firms are now offering "data lockers". These allow users to contribute and edit the data they are willing to share

---

[145] Alessandro Acquisti, Leslie K John, and George Loewenstein, *What is Privacy Worth?* 42 The Journal of Legal Studies 249-274 (2013).

[146] Kai-Lung Hui and IPL Png, *The Economics of Privacy* in T Hendershott (ed), *Handbook on Economics and Information Systems,* 471-498 (Amsterdam, 2006).

[147] Spiekerman et al (n 146), 38-47.

[148] See e.g., Paul Rubin and Thomas Lenard, *Privacy and the Commercial Use of Personal Information* (Springer 2002).

[149] OECD *Economics of Personal Data* (n 135) 30, citing studies by Norbert Schwarz, *Self-reports: How the Questions Shape the Answers* 54 American Psychologist (1999); Acquisti et al (n 148), 249-274.

[150] Acquisti et al (n 148), 249-274.

[151] OECD *Economics of Personal Data* (n 135), 4-5.

with third parties in exchange for a portion of the proceeds when their data is sold.[152] These data lockers could potentially improve transparency about how data is collected, sold and used. Users may be willing to share more personal data if they feel they have more control over how it is used and receive a clear economic or social benefit in exchange for sharing. Consequently, sales prices through "data lockers" might become a key method for valuing personal information and privacy.[153] This is a new area and although it is unclear if data lockers will emerge with viable business models, this is an area worth following up in the privacy context.

Further, the EU's proposal on digital taxation reflects some elements that bear interesting similarities to the discussion on measuring privacy harm by looking at the number of users. In the EU tax reform proposal, the Commission proposes new measures to ensure that digital business activities are taxed fairly in the EU.[154] The initiative aims to reform corporate tax rules so that profits are registered and taxed where businesses have significant interaction with users through digital channels. Consequently, one of the criteria for considering a digital platform as having a taxable "digital presence" or a virtual permanent establishment in an EU Member State is that it has more than 100,000 users in a Member State in a taxable year. (Another alternative criterion is that a digital platform has more than 3000 business contracts for digital services created between the company and business users in a taxable year.)

Further to the question of valuation of personal data, it should be noted that related issues often arise in the context of two-sided advertising supported markets, which brings about challenges in terms of how to balance possible benefits on the "paid" advertising side of the market against harms on the "free" consumer side of the market, as seen in *Facebook/WhatsApp* and *Google/DoubleClick*. What makes it even more difficult is that situations arise in the digital economy where protection of privacy can both enhance and detract from individual and societal welfare.[155] Another challenge is that consumers' ability to make informed decisions about their personal information and privacy is hindered because they are often in a position of imperfect information about when their data is collected, for what purpose, and with what consequences.[156] In addition, consumers' concern for their data protection can also be distorted by other factors, such as the power of defaults[157] and the "free effect".[158]

The phenomena highlighted and discussed above may contribute to the existing privacy paradox, namely that while many users are concerned about privacy, few

---

[152] *Ibid.*, 5.

[153] *Ibid*.

[154] Commission press release, 'Digital Taxation: Commission Proposes New Measures to Ensure That All Companies Pay Fair Tax in the EU' (Brussels, 21 March 2018).

[155] Alessandro Acquisti, Curtis R Taylor and Liad Wagman, *The Economics of Privacy* 52 Journal of Economic Literature 2 (2016).

[156] *Ibid*.

[157] Ezrachi and Stucke (2016) (n 10), 35.

[158] Gal and Rubinfeld (n 109), 530.

actually act on those concerns.[159] Nevertheless, those few privacy-aware consumers that do value data protection are enough to raise competitive concerns. As mentioned, privacy is subjective, meaning that not all consumers value the same things, and privacy might affect marginal consumers who are those to keep market power in check.[160] In this context, it is noteworthy that consumers' views on the value of personal data may be shifting in the wake of the Facebook-Cambridge Analytica scandal and users are likely becoming more attentive to privacy, and perhaps the Cambridge Analytica affair may even be remembered as the beginning of a larger reckoning. Even Facebook's CEO Marc Zuckerberg has said that new regulation is "inevitable."[161]

Further to the privacy paradox, which reflects irrational consumer behaviour, consumers can behave irrationally in other ways in the context of digital markets, often because they are lured by free services, the so called free effect.[162] For example, the power of default, an idea stemming from behavioural economics, makes consumers stick to the default option not just due to the practices of the dominant company but also because of an artificial lock-in effect. This means that consumers sometimes prefer to stick to the default option, even if faced with better or higher quality alternative options, because they feel comfortable and do not want to experience additional learning costs.[163] This phenomenon can also be referred to as consumers experiencing "high switching costs".[164] A key point with the power of the default option is that this notion from behavioural economics, which often stands in contrast to the approach of traditional law and economics, can help explain the market power of dominant companies in online markets and the presence of barriers to entry. Dan Ariely, an expert in applied behavioural economics, captures the problem with privacy and the irrational behaviour of consumers in the following question:

> *Wouldn't economics make a lot more sense if it were based on how people actually behave, instead of how they should behave?*[165]

---

[159] Francisco Costa-Cabral and Orla Lynskey, *Family Ties: The Intersection Between Data Protection and Competition in EU Law* 54 Common Market Law Rev 28 (2017).

[160] *Ibid.*, 28.

[161] Aaron Pressman, 'Facebook Can't Fix this Problem Alone' in *Fortune* (20 April 2018) <http://fortune.com/2018/04/20/facebook-data-privacy-problem-fix/> accessed 5 March 2019.

[162] Gal and Rubinfeld (n 109), 530.

[163] E.g., consider the current *Google Android* case in the EU. Commission Decision of 18 July 2018 relating to proceedings under Art. 102 TFEU and Art. 54 Agreement on the European Economic Area AT.40099.

[164] On switching costs, see e.g., Aaron S Edlin and Robert G Harris, *The Role of Swicthing Costs in Antitrust Analysis: A Comparison of Microsoft and Google* 15 Yale Journal of Law and Technology 169-213 (2013).

[165] Dan Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions* (HarperCollins, New York, 2008).

VI. Conclusions

This article has highlighted the increasing role and importance of data and privacy in competition law, especially in the area of merger control considering the number of data-driven acquisitions in digital markets. The aim of this article is to contribute to the ongoing debate concerning the complex relationship between the two legal areas of competition and data protection. Many of the issues raised here relate to broader policy questions and themes that go beyond the scope of this brief article and deserve further research.[166] Suffice to say here that with increasing attention devoted to the competition-privacy interface, not only in academia but also by the leading competition authorities, the conventional hard line between competition law and privacy may be softening and there is a clear need to develop adequate policy responses.

With the rise of data-driven mergers, competition authorities will increasingly have to confront data and privacy implications in their competitive assessment. The conditional *Microsoft/LinkedIn* merger decision, the developments concerning privacy degradation in the case of Facebook, and the recent *Apple/Shazam* merger decision, all go to support the observation that competition enforcers are becoming more sensitive to the role of data and privacy protection in their competition review. While the overall principles may be similar for the competitive assessment of data-driven mergers, they will require more sophisticated analysis of the nature of transactions with customers and the effects of two- or multisided markets to identify the actual price paid in terms of lost privacy.

To address some of these challenges of dealing with personal data and privacy, this article points to some relevant methodologies to estimate or assign monetary values to personal data with the idea that such methods could be used as basis to further develop the economic and legal analysis of privacy with the ultimate aim of creating a measuring tool for competition authorities. In practice, however, this will likely be a challenging task and may necessitate both an intellectual and policy shift to adequately take into consideration and effectively measure the ever-important non-price elements of competition. This article hopefully offers food for thought on the way.

---

[166] The author explores this topic in a paper *EU Competition Policy for the Digital Economy*, forthcoming in issue 24.3 of in Columbia Journal of European Law, and as part of her doctoral thesis in law.